Bayalink Liberty R1.7 and R2.0

Security and Deployment Overview

Feb. 1, 2009

©2009 Bayalink Solutions Corp.. All Rights Reserved. The Bayalink and Bayalink Liberty families of related marks, images, and symbols are the exclusive properties of Bayalink Solutions Corp..

This document is provided “as is” and Bayalink Solutions Corp. assumes no responsibility for any typographical, technical, or other inaccuracies in this document. Bayalink Solutions Corp. reserves the right to change information contained in this document without notice.

The Citrix, Outlook, Outlook Web access, BlackBerry and RIM families of related marks, images, and symbols are the exclusive properties of their respective owners.

Overview of Bayalink Liberty™

Bayalink Liberty is referred to as an application virtualization technology for popular smartphones, most notably the BlackBerry® from Research in Motion Ltd.. Bayalink Liberty works by creating a Container on the endpoint PC which we refer to by various names: Liberty Viewer, Liberty Application, or just Liberty and we attach securely to this Container from the handheld over Bluetooth or USB tether.

Within the Container the Liberty Viewer securely renders smartphone application data but in a layout that is more suitable for productivity on a PC form factor. For example, our email client takes advantage of multiple windowing, a folder tree viewer and other features that make reading, creating and sending email via your smartphone far more productive than from your handheld alone. Further, regarding email, we provide full featured native attachment access via the handheld's communications infrastructure.

The Container is actually comprised of a number of software components that provide the overall functionality of rendering specific smartphone applications (the data) to the Liberty Viewer.

Liberty endpoint architecture (Container components):

Liberty Monitor: The Liberty Monitor is the control centre of the Liberty software that runs on the endpoint. It is responsible for primitive status indications to the User, initial setup and pairing with the handheld and, it coordinates and monitors the other processes.

Liberty Key and Bluetooth driver: The Liberty Key software is initially loaded and controlled by the Liberty Monitor software. The Liberty Key interfaces with our proprietary Bluetooth stack that allows pairing to the Liberty USB Key enabling the USB Key to be plugged into any endpoint without pairing again. The pairing requires the user to choose a random pass code that is entered both on the handheld and the initial endpoint used for setup. Subsequent connections, regardless of endpoint, are thus encrypted with a standard 128bit private key cipher between the handheld and the Liberty Key. This security feature is comparable to having a password on the handheld and requiring that the password be entered when the handheld is tethered via the USB cable. The Liberty Key software also supports a USB tethered connection and enforces password authentication if required by the handheld's IT policy.

Liberty Core: The Liberty Core is also initially loaded and controlled by the Liberty Monitor. The Liberty Core is a Java based server that accepts the connection request from the Liberty handheld software (Liberty HD) only after the Liberty Key software has established the SPP connection and makes a bridge to the Liberty Core. Once the bridge to the Liberty Core is established an authenticating handshake between the Liberty HD software and the Liberty Core is made. As part of the handshake dialog the Liberty Core will only allow requests for handheld resources from authenticated clients. In particular, once the handshake is complete the Liberty Core launches the Liberty Viewer application and it is the only application capable of accessing handheld resources via the Liberty Core. The Liberty Core provides its HTTP proxy services and its handheld services by listening on a number of localhost ports:

Copyright 2009 Bayalink Solutions Corp.

Port 3125 – Serves handheld resource calls such as sending and receiving email, making phone calls, updating the calendar, etcetera. This is the primary port used by the Liberty Viewer.

Port 3126 – Provides HTTP proxy services on the Carrier or WiFi direct backbones. **NOTE**: this can be disabled through enterprise IT Policy.

Port 3127 - Provides HTTP proxy services on the BES/MDS backbone enabling secure access to intranet resources and applications.

Port 3128 – A special port that allows the Liberty Viewer to establish secure Remote Desktop connections to computers running behind the firewall in the enterprise or to servers on the Internet as specified by the User.

NOTE: The Liberty Core implements a lightweight firewall that will only allow connections to these ports from the local machine and in the case of connections on 3125, as mentioned, it only allows connections from the Liberty Viewer.

Handheld data store access

The latest handhelds have many gigabytes of storage available via removable microSD card technology. Enterprises concerned with security while compelled to enable their User community to take advantage of this storage should apply a rigid data security policy. Generally the storage should be encrypted since it is removable. Further it is recommended that Mass Storage Mode not be enabled for the flash drives. By allowing mass storage mode the enterprise exposes the possibility of corporate data being compromised when the handheld is connected to an un-trusted endpoint.

Bayalink Liberty provides secure access to the handheld file stores and makes them available through Liberty via its Virtual File System technology.

Virtual File System (VFS) services are provided by the Liberty Core and allow the Viewer, browsers, and Windows Explorer to access the data stores of the handheld in a controlled and secure way. Enterprises can enable their users for flash storage use, enforce data encryption and turn off mass storage capabilities yet still allow secure access to the flash storage resources via the Liberty VFS facility. The VFS can be configured by IT Policy, or by the handheld options otherwise, to set the level of control and restrictions to the handheld's file system. As an example you can allow VFS access via the Browser but not the File Explorer or vice verse, you can require a challenge for authentication when a browser or the File Explorer attempt to connect to the VFS, among others.

Data Residuals and Leakage

In many deployment scenarios (mostly those where Liberty is being used on an endpoint that is not the User's own trusted computer: such as in a lounge or on a plane etcetera) concerns about data being left behind on the endpoint (Data Residuals) and data unknowingly being "scraped" and sent over the Internet (Data Leakage) are well understood.

Copyright 2009 Bayalink Solutions Corp.

Bayalink provides two approaches to protecting the unsuspecting user from data residuals and data leakage.

1. R1.7 provides data residual protection with File System Monitor (FSM) technology. When enabled by the User, the FSM will track all changes to the endpoint file systems during a Liberty session and will prompt the User to clear the changes that are unwanted at the end of the Liberty session.

2. R2.0 provides data residual protection and data leakage protection using our Data and Network Container technology. With 2.0, the User logs into the endpoint to begin a Liberty Session and all changes to the endpoint are contained and later cleared automatically at the end of a Liberty Session. Data that needs to persist must be saved to the handheld via the VFS. Further, with the Network Container technology, during a Liberty Session all network interfaces on the endpoint are disabled and remain disabled during the session. The only network access is via the Liberty proxy, through the enterprise, when the Network Container is enabled. With R2.0 the enterprise has a number of options to control the handheld and the endpoint with respect to data management.

Application Overview

In Liberty R1.7 the applications are: Email, Calendar, Contacts, Browser, Phone, Virtual File System (VFS), and Remote Desktop (RDP).

An overview of the feature functionality of the various applications is below:

Email:

- Full desktop-like email functionality
- Native attachment downloading
- Sending native attachments in new messages

Considerations:

- Liberty does not synchronize email with the endpoint it is a pure transient image of the email on your handheld. When the Liberty session ends no email is ever left anywhere on the endpoint
- Native attachments can be accessed in 1 of 3 ways in release 1.7:

    1. Using our hosted facility you can setup a mirror account on our servers and when the attachment is requested the email containing the attachment is forwarded to our server and the Liberty Viewer pokes into that server and retrieves the attachment on the User's behalf. This is suitable for Prosumer User's comfortable with using our third-party service. Your email does reside on our server for a period

Copyright 2009 Bayalink Solutions Corp.

of time while the attachment is being retrieved. Clearly for enterprises this alternative is not likely to pass information security policy.

2. Using our enterprise attachment service, enterprises can install our server behind their firewall. In this way no email is ever forwarded outside of the corporate "wall". The Liberty Viewer is simply configured to use the standard BES/MDS conduit to securely access the attachment server and retrieve the requested attachment. Our enterprise attachment server requires that you configure your email server to allow IMAP connections. This DOES NOT require that you open IMAP on your firewall! You could also choose to either install the EBAS server on the same server(s) as the email server or configure the link between the EBAS server and the email server using secure IMAP if you are concerned about sniffing on your internal network backbone.

3. Using the "Download Attachment" features of the latest BlackBerry systems the User can select to download the desired attachment to their handheld's internal store of choice. Once the attachment is downloaded to the handheld in its native format, the User can access the attachment on the endpoint via Liberty's secure VFS technology. The VFS link between the endpoint Liberty Container can be further secured by an authentication challenge to ensure only the User is accessing this attachment via Liberty versus some, albeit unlikely, virus running on the endpoint. NOTE: with our R2.0 Data Container platform, even this unlikely scenario of endpoint viruses are contained by only allowing data i/o via Liberty to the handheld.

Calendar:

- Full desktop-like calendar functionality
- Creating new appointments are immediately reflected on the handheld
- Inviting others by integrating with the Contacts list

Considerations:

- Liberty does not synchronize calendar information with the endpoint. It is a pure transient image of the calendar on your handheld. When the Liberty session ends no calendar information is ever left anywhere on the endpoint

Contacts:

- Full desktop-like address book functionality
- Creating, editing, deleting and emailing from the Contacts List
- Server side address book lookup

Copyright 2009 Bayalink Solutions Corp.

- Integrated with the email and calendar functions

Considerations:

- Liberty does not synchronize contact information with the endpoint. It is a pure transient image of the address book on your handheld. When the Liberty session ends no address book information is ever left anywhere on the endpoint

Browsing:

- Full HTTP 1.1 compliant browsing using industry standard browsers
- TLS/SSL 3.0 for full internet-based security
- Access to intranet web applications via BES/MDS
- Access to remote file systems via WebDAV services
- Proxy authentication and dynamic proxy script support
- ISA and NTLM compatible

Considerations:

- Since the link between the Liberty HD component and the Liberty Key component is secure (whether using Bluetooth or a tethered USB connection), the entire pipe from the Browser, to the Liberty proxy, to the handheld, through the BES/MDS infrastructure to the target intranet server is secure.
- Because of the full HTTP 1.1 compliancy, access to Internet resources are secure using standard TLS/SSL3.0 technologies as if you were browsing from any desktop using any ISP.
- Cookies and browsing history are either manually cleared with R1.7 or automatically contained with R2.0 as described above.
- If using Firefox from the Liberty USB Key all history and cookies can be retained for convenience on the USB key store if desired.
- NOTE: Future releases will have a capability to persist cookies and history back to the handheld so that a User can maintain their Browser settings regardless of the endpoint they are using if desired.

Phone:

- Allows accepting and placing phone calls through the handheld while remaining in a Liberty Session

Copyright 2009 Bayalink Solutions Corp.

- Call direct from Contact List

Considerations:

- This feature requires Input Simulation/Key Injection permissions be granted to the Liberty HD application

Virtual File System I:

- First generation of the VFS allows:
    - Access to the stores of the handheld via Browser or File Explorer with Mass Storage Mode off on the handheld
    - Access to remote file systems behind the firewall on servers configured with WebDAV mounts

Considerations:

- Compliancy with proxies behind the firewall for remote file system access such as ISA
- integrated NTLM authentication capable
- Leverages secure BES/MDS for remote file access
- Containment (see Data Residuals and Data Leakage above) is the same as if the file was retrieved as an attachment from an email

Remote Desktop (RDP):

- Liberty keeps a list of named servers that can be found behind the firewall via BES/MDS or exposed on the Internet
- Liberty provides a specialized RDP proxy that enables the endpoint RDP client to connect to one of the selected servers from the named list. If the RDP proxy can connect to the server it establishes a tunnel and hands off the connection to the endpoint's RDP client

Considerations:

- Using an RDP session to access remote resources makes data containment a non-issue at the endpoint

Copyright 2009 Bayalink Solutions Corp.

Conclusion

At Bayalink we believe the handheld is the final frontier for your data. Why would you want or need yet another copy of your data? Having more copies of your data is completely counter to what enterprises are trying to achieve which is a managed, holistic view of their data and eliminating data sprawl. Clearly, it's what any User would want as well – their data in one spot.

Whether you are Joe's Plumbing and HVAC or the NSA Bayalink has an endpoint independent mobility platform that can reduce complexity of your infrastructure, reduce costs of facilities, increase productivity, and align to your corporate IT security policies.

We invite you to contact us to discuss how the Bayalink Liberty solution can work for you.

Copyright 2009 Bayalink Solutions Corp.